Reference: Notification of a data breach pursuant to Art. 34 of the General Data Protection Regulations {GDPR] (DSG-VO)

Dear Sir / Madam,

On 29 March we noted that the IT systems of Lomberg GmbH were affected by an IT security incident. Today we are able to confirm that it is a criminal ransomware attack. Consequently we would like to submit more detailed information concerning the fact that your personal data may possibly have been compromised.

The current status of investigations shows that the hackers obtained unauthorised access to internal business information and to personal data and they have encrypted it.
On 21 April 2022 the hackers published various data in the darknet. There is likewise the risk that confidential information may continue to be offered for sale, even if the aim of these criminal acts may well primarily have been the disruption of business operations.

Taking into consideration the financial risks and other possible losses, we have not complied with the hackers‘ demand for the payment of ransom money. We shall not do so in future either.

When we found out about the incident, we took down all servers from the internet immediately to protect our systems, and to prevent subsequent unauthorised access. We have appointed specialist forensic experts and cyber security experts to investigate the incident, to restore data from back-ups and to enhance the security of our systems. In addition to this, we have heightened the awareness of our employees to the significance of cyber security and we shall continue to expand our cyber security training courses.

For the purposes of transparency and in accordance with Art. 34 of the General Data Protection Regulations, we wish to take this opportunity to inform you that your personal data is also saved in our system and this means that you too could be affected by this security breach.

Since we can unfortunately not rule out that your data has also been compromised, and that it is therefore possible that you are at risk of identity theft, fraud, financial loss, loss of control over your personal data, or social disadvantage, we would recommend that you consider the following measures to protect your personal data:

1. Change your passwords
2. Raise your employee awareness concerning cyber security
3. Inform your banks and other financial institutions of the potential risk to your accounts from unauthorised activities.
4. Check your electronic communications for suspicious messages.

By taking measures immediately we have managed to limit the potential for damage to a low level and secure our ability to supply the bulk of our product range. We managed to start up our important systems, goods handling systems, logistics management, the interfaces to our banks and many security-related systems again at short notice within a few days. We have also managed to make progress in securing our systems and their data and we shall be fully operational again very soon. We would like to apologise for any delays in delivery there may be. We should also like to apologise for the eventuality that you receive the same invoices or order confirmations or other automated documents twice. Should you have any questions concerning this we would ask that you get in touch with your contact in our company.

You can contact our data protection officer concerning data protection law matters at the following address:

Riske IT GmbH
Herr Pascal Riske
Keldenicher Straße 23
50389 Wesseling
Web: www.riske-it.de
E-mail: datenschutz@riske-it.de

Please appreciate that in view of the complexity of the investigations at the present point in time, we are unable to disclose any further information about the incident. We shall be in touch again once we have further relevant information.

We regret that this incident has occurred and all the unpleasantness you may possibly have suffered as a result. Please be assured that the security of our systems and your data is our top priority.